CLAIMS

1. A processing system comprising a central processor, a BIOS memory device and a BIOS protection device interconnected by address and data paths, wherein at start-up, the BIOS protection device takes control of the memory address and data paths and prevents execution of a boot program stored in the BIOS memory device until the BIOS protection device has verified that the boot program stored in the BIOS memory device is authentic.

2. The system as claimed in claim 1 wherein the BIOS protection device is connected to the processing system between a central processor and the BIOS memory device, the BIOS protection device including address and data path interface connection means, and an authentication processor whereby, when power is applied to the BIOS protection device, the BIOS protection device takes control of address and data path(s) to which it is connected and the authentication processor interrogates the BIOS memory device connected to the address and data path(s) to determine if the boot program contained in the BIOS memory device is authentic, and only if the boot program is determined to be authentic does the BIOS protection device release control of the address and data path(s) to permit the central processor to execute the boot program.

3. The system as claimed in claim 2 wherein the address and data path interfaces comprise one of a serial interface, a totally non-multiplexed bus, an Intel™ Low Pin Count (LPC) bus structure.

4. The system as claimed in claim 2 wherein the address and data path interfaces comprise an Intel™ Low Pin Count (LPC) bus structure.

5. The system as claimed in claim 1, 2, 3 or 4 wherein the BIOS memory device includes a cryptographic digital signature located at a known location in the BIOS memory device.

6. The system as claimed in claim 5 wherein the BIOS protection device calculates the value of the cryptographic digital signature from contents of the BIOS memory device and an internal public key and interrogates the BIOS memory device to verify that the correct signature is present and corresponds with the boot program, or a part thereof stored in the BIOS memory device.

7. The system as claimed in any one of claims 1 to 6 wherein the BIOS protection device also contains an internal memory device and while authenticating the BIOS contents, the BIOS protection device copies at least part of the BIOS memory device contents to the internal memory device and subsequently controls the address and data path(s) to bypass the BIOS device and communicate with the internal memory device

instead when the central processor attempts to access the copied part of the BIOS memory device contents.

8. The system as claimed in any one of claims 1 to 7 wherein the central processor, the BIOS memory device and the BIOS protection device are mounted on a motherboard on which at least one signal line of the motherboard is interrupted by the BIOS protection device such that the motherboard is inoperative if the BIOS protection device is not present.

9. The system as claimed in claim 8 wherein a reset control circuit is provided in the BIOS protection device such that the mother board cannot exit the reset state if the BIOS protection device is not present.

10. The system as claimed in claim 9 wherein the BIOS protection device will hold the reset signal in the reset (or, disabled) state while the authentication of the BIOS is performed.

11. The system as claimed in claim 10 wherein when the authentication is successful, the BIOS protection device releases the reset signal allowing the central processor to commence operation.

12. The system as claimed in any one of claims 1 to 8 wherein the BIOS protection device inserts wait cycles to disable the central processor while authenticating the BIOS memory device.

13. A method of authenticating a boot program held in a BIOS memory device of a processing system comprising a central processor, the BIOS memory device and a BIOS protection device interconnected by address and data paths, the method comprising the steps of:

1) at start-up, the BIOS protection device temporarily prevents execution of the boot program by the central processor;

2) the BIOS protection device takes control of the address and data paths;

3) the BIOS protection device interrogates the contents of the BIOS memory device to establish if the contents are authenticated;

4) if the contents of the BIOS memory device are not authentic, the BIOS protection device continues to prevent execution of the boot program and prevents further operation of the central processor ; and

5) if the contents of the BIOS memory device are authentic, the BIOS protection device relinquishes control of the address and datapaths and allows the central processor to execute the boot program in the BIOS memory device.

14. The method as claimed in claim 13 wherein the address and data paths are interfaced via one of a serial interface, a totally non-multiplexed bus, an Intel™ Low Pin Count (LPC) bus structure.

15. The method as claimed in claim 14 wherein the address and data paths are interfaced via an Intel™ Low Pin Count (LPC) bus structure.

16. The method as claimed in claim 13, 14 or 15 wherein a cryptographic digital signature is provided at a known location in the BIOS memory device .

17. The method as claimed in claim 16 wherein the value of the cryptographic digital signature is calculated by the BIOS protection device from contents of the BIOS memory device and an internal public key and the BIOS protection device interrogates the BIOS memory device to verify that the correct signature is present and corresponds with the boot program, or a part thereof stored in the BIOS memory device.

18. The method as claimed in any one of claims 13 to 17 wherein the BIOS protection device also contains an internal memory device and while authenticating the BIOS contents, the BIOS protection device copies at least part of the BIOS memory device contents to the internal memory device and subsequently controls the address and data path(s) to bypass the BIOS device and communicate with the internal memory device instead when the central processor attempts to access the copied part of the BIOS memory device contents.

19. The method as claimed in any one of claims 13 to 18 wherein the central processor, the BIOS memory device and the BIOS protection device are mounted on a motherboard on which at least one signal line of the motherboard is interrupted by the BIOS protection device whereby the motherboard does not perative when the BIOS protection device is not present.

20. The method as claimed in claim 19 wherein a reset control circuit is provided in the BIOS protection device whereby the mother board does not exit the reset state if the BIOS protection device is not present.

21. The method as claimed in claim 20 wherein, while the authentication of the BIOS is performed, the BIOS protection device holds the reset signal in the reset (or, disabled) state.

22. The method as claimed in claim 21 wherein, when the authentication is successful, the BIOS protection device releases the reset signal and the central processor commences operation.

23. The method as claimed in any one of claims 13 to 19 wherein the BIOS protection device inserts wait cycles to disable the central processor while authenticating the BIOS memory device.

24. A BIOS protection device for connection to a processing system between a central processor and a BIOS memory device containing a boot program, the BIOS protection device including address and data path interface connection means, and an authentication processor whereby, when power is applied to the BIOS protection device, the BIOS protection device takes control of address and data path(s) to which it is connected and the authentication processor interrogates the BIOS memory device connected to the address and data path(s) to determine if the boot program contained in the BIOS memory device is authentic, and only if the boot program is determined to be authentic does the BIOS protection device release control of the address and data path(s) to permit the central processor to execute the boot program.

25. The device as claimed in claim 24 wherein the address and data path interfaces comprise one of a serial interface, a totally non-multiplexed bus, an Intel™ Low Pin Count (LPC) bus structure.

26. The device as claimed in claim 25 wherein the address and data path interfaces comprise an Intel™ Low Pin Count (LPC) bus structure.

27. The device as claimed in claim 246, 25 or 26 wherein the BIOS memory device includes a cryptographic digital signature located at a known location in the BIOS memory device.

28. The device as claimed in claim 27 wherein the BIOS protection device calculates the value of the cryptographic digital signature from contents of the BIOS memory device and an internal public key and interrogates the BIOS memory device to verify that the correct signature is present and corresponds with the boot program, or a part thereof stored in the BIOS memory device.

29. The device as claimed in any one of claims 24 to 28 wherein the BIOS protection device also contains an internal memory device and while authenticating the BIOS contents, the BIOS protection device copies at least part of the BIOS memory device contents to the internal memory device and subsequently controls the address and data path(s) to bypass the BIOS device and communicate with the internal memory device instead when the central processor attempts to access the copied part of the BIOS memory device contents.

30. The device as claimed in any one of claims 24 to 29 wherein the central processor, the BIOS memory device and the BIOS protection device are mounted on a motherboard on which at least one signal line of the motherboard is interrupted by the

BIOS protection device such that the motherboard is inoperative if the BIOS protection device is not present.

31. The device as claimed in claim 30 wherein a reset control circuit is provided in the BIOS protection device such that the mother board cannot exit the reset state if the BIOS protection device is not present.

32. The device as claimed in claim 31 wherein the BIOS protection device will hold the reset signal in the reset (or, disabled) state while the authentication of the BIOS is performed.

33. The device as claimed in claim 32 wherein when the authentication is successful, the BIOS protection device releases the reset signal allowing the central processor to commence operation.

34. The device as claimed in any one of claims 24 to 30 wherein the BIOS protection device inserts wait cycles to disable the central processor while authenticating the BIOS memory device.